

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF:

One (1) Alienware Laptop displaying product key: CY96D-3PVJ8-
2Y7WF-3G4WJ-GQB8

Magistrate No.
[UNDER SEAL]

LOCATED AT FBI PITTSBURGH, AT 3311 E CARSON ST,
PITTSBURGH, PA 15203

19.0869M

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Katherine Donohue, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), assigned to the Pittsburgh, Pennsylvania office. I have been employed as a Special Agent for the FBI since June 2016. As part of my duties, I investigate violations of federal law, including the online exploitation of children, including violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have gained expertise in the conduct of such investigations through training in the area of child pornography and child exploitation investigations in seminars, classes, and everyday work related to conducting these types of investigations and have had the opportunity to observe and review numerous examples of child pornography in a variety of media, including computer media. I have obtained FBI Basic and Advanced Crimes Against Children Training. I have participated in the execution of numerous federal and state search warrants which have involved child sexual exploitation and/or child pornography offenses. By virtue of my position, I perform

and have performed a variety of investigative tasks, including the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. I have personally participated in the execution of numerous federal search warrants involving the search and seizure of computer equipment in cases involving violations of Section 2252(a).

2. This affidavit is made in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession (at FBI Pittsburgh), and the extraction from that property of electronically stored information described in “Attachment B.” The Target Device is specifically described in “Attachment A.”

3. The purpose of this application is to seize evidence, fruits, and instrumentalities, more particularly described in Attachment B, of violations of Title 18, United States Code, Section 2422(b), which makes it a crime to use a facility and means of interstate commerce, such as the Internet and the telephone, to attempt to knowingly persuade, induce, and entice an individual who has not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense, and violations of 2252(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor, and violations of Title 18, United States Code, Section 2252(a)(4)(B), which makes it a crime to possess material depicting the sexual exploitation of a minor and access with intent to view it, and Title 18, United States Code, Section 2251(a), which makes it a crime to produce material depicting the sexual exploitation of a minor (child pornography).

4. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines “minor”, for purposes of Section 2252, as “any person under the age of eighteen years.” Section 2256 also defines “sexually explicit conduct” for purposes of these

sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic; or (e) lascivious exhibition of the genitals or pubic area of any person.

5. The statements in this affidavit are based, in part, on information provided by witnesses and your affiant's investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2422(b), 2251(a), 2252(a)(2) and 2252(a)(4)(B) are presently located on evidence held at FBI Pittsburgh. I request authority to search the entirety of the Target Device, for the items specified in Attachment B, hereto, which items constitute fruits, instrumentalities, and evidence of the foregoing violations.

6. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers and other personnel specially trained in the seizure and analysis of computers and electronic mobile devices and electronic storage devices, and on my experience and training as a federal agent.

7. In summary, the following affidavit sets forth facts that establish that there is probable cause to believe that Thomas STULTZ, enticed, persuaded, and induced a minor, as well as received, and/or possessed visual depictions of minors engaged in sexually explicit conduct, using an electronic device, presently located at FBI Pittsburgh, to produce and access said materials.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

8. The property to be searched is described as follows: Alienware laptop displaying product key: CY96D-3PVJ8-2Y7WF-3G4WJ-GQB8.

9. The device is currently located at the Federal Bureau of Investigation (FBI), 3311 E Carson St, Pittsburgh, PA 15203.

10. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

11. Between the dates of January 28, 2019 and February 1, 2019, the undercover agent created an account on the Internet-based application Grindr. Grindr is a geosocial networking and online dating application geared towards gay and bisexual individuals. It runs on iOS and Android devices, and is available for download from the Apple App Store and Google Play. Users can tap on the picture of another Grindr user, and the app will display a brief profile for that user, as well as the option to chat, send pictures, and share one's precise location.

12. In this investigation, the undercover assumed the identity of a fourteen-year-old male located in Pittsburgh, Pennsylvania. An individual with the Grindr username "darkzero" contacted the undercover via the app and engaged the undercover in a private messaging conversation on February 6, 2019 at or around 10:41 AM. Between the dates of February 6, 2019 and February 27, 2019, Grindr user "darkzero" contacted the undercover several times via private chat on Grindr, and they continued to communicate thereafter via phone to phone text messages.

13. User "darkzero" has a profile picture on his Grindr profile and, during chats with the undercover, "darkzero" provided the telephone number (724)321-2360 as his telephone

number and advised his name was “Tom”. On February 6, 2019, investigators linked telephone number (724)321-2360 to THOMAS PERRY STULTZ of 601 Bellevue Terrace, Pittsburgh PA, 15202 via open source checks. During a text message chat with the undercover on February 20, 2019, at approximately 2:09 PM, “darkzero” sent an image of his residence in which the street sign next to his house is visible. The street sign in the image reads: “Bellevue.” The image also depicts a red brick building with a green awning. Law enforcement surveillance confirmed this description of the location at 601 Bellevue Terrace, Pittsburgh PA, 15202. Based on this, law enforcement believe Grindr user “darkzero” is THOMAS PERRY STULTZ living at 601 Bellevue Terrace, Pittsburgh PA, 15202.

14. On February 6, 2019 the undercover, pretending to be a 14 year old boy, told “darkzero” that he was supposed to be in school, and he was skipping class. Almost immediately after initiating the conversation with the undercover, STULTZ asked the undercover to send him (STULTZ) a picture of himself: “Can I see what your bad self looks like?” STULTZ told the undercover that if he sent him a picture, he (STULTZ) would “jerk off to it.” STULTZ then sent six images that STULTZ stated were of himself: three of which depicted his erect penis, and one of which displays ejaculation on his bare chest and stomach. In this conversation, STULTZ asked the undercover: “Can you cum yet?”, and then commented: “Just starting to maybe?”, indicating that STULTZ believed that the individual with whom he was communicating was under the age of eighteen.

15. After STULTZ sent the undercover pictures of himself, STULTZ told the undercover: “I would love to see how your naughty bits look” and that they could do that “In person or on pic.” When the undercover asked: “How would do in person? I mean would you go slow”, STULTZ responded: “I definitely would. You’re really new and I’d rather have fun

teaching you.” In the course of the conversation, STULTZ clarified: “I would like to first get us naked so that we could explore each other’s bodies.” STULTZ subsequently asked: “How old are you btw [by the way]?” The undercover stated: “14; Hbu?” (in the context of texting, “hbu” means: how about you), to which STULTZ replied “nice”, and then provided that his age is “36” (years old).

16. STULTZ continued to engage the undercover and discuss how they could meet on a day when the minor (undercover) skipped class. As they discussed good days to meet, the following conversation took place between STULTZ and the undercover:

02/06/2019 11:57 AM – STULTZ – So, just curious, but did you want to get penetrated?

02/06/2019 11:57 AM – STULTZ – YES!! Monday would work fine

02/06/2019 11:59 AM – UC – If you use lube

02/06/2019 11:59 AM – STULTZ – Oh for sure I would

02/06/2019 11:59 AM – STULTZ – Do you want me to wear a condom?

02/06/2019 12:00 PM – UC – When youre inside me yeah. Kinda nercous without

02/06/2019 12:00 PM – STULTZ – I understand. Although I get tested regularly and I’m on prep

02/06/2019 12:00 PM – UC – What’s prep

02/06/2019 12:01 PM – STULTZ – It’s called truvada. It’s the HIV vaccine

02/06/2019 12:01 PM – UC – Oh. Thats a really good idea

02/06/2019 12:02 PM – STULTZ – Mmhmmmmmm. It’s free lol

02/06/2019 12:03 PM – STULTZ – So, I’m protected from the worst of them lol

02/06/2019 12:04 PM – UC – Hehe

02/06/2019 12:04 PM – STULTZ – In addition to being a top and not getting around all that much at all, I've never had a disease

02/06/2019 12:04 PM – UC – That's good. Cuz I don't want any disease

02/06/2019 12:05 PM – STULTZ – I don't want to give you and either

STULTZ also asked the undercover to send (to STULTZ) an image of himself. The undercover sent a sanitized image (no face) of another law enforcement officer taken when the officer was approximately 14 years old. In the picture, the boy is wearing swimming trunks with no top. Upon receipt of the image, STULTZ replied "Oh geez. Hell yes", "you're sexy af" (af in this context is understood to be "as fuck").

17. Eventually, STULTZ and the undercover agreed to transition their communications from Grindr to phone to phone text messages when the undercover told STULTZ that he usually deletes his apps when he goes home so that his mom does not see them. At that point, STULTZ sent the undercover his phone number: 724-321-2360 and told the undercover to save his number under the name "Tom".

18. After transitioning to phone texting, the undercover and STULTZ had the following conversation about the picture the undercover sent purporting to be the 14 year old boy:

02/06/2019 12:46 PM – STULTZ – Btw. I keep looking at that pic

02/06/2019 12:46 PM – STULTZ – I love your bellybutton

02/06/2019 12:46 PM – UC – Hehe. Why the bellybutton?

02/06/2019 12:47 PM – STULTZ – Well, not only that, your nipples also, but I like to lick around the belly

02/06/2019 12:49 PM – UC – What else

02/06/2019 12:49 PM – STULTZ – Well, suck on your nipples while cupping your balls and peep. Kiss your neck and lick in your ear. Roll you over and kiss down you back until I get to that little butt. Then I'll run it and kiss and lick all over it and down to you balls

19. In this conversation, and on another occasion, STULTZ made plans to meet the minor (undercover). Neither of these meetings ultimately occurred. When STULTZ failed to finalize the first meeting (tentatively set for February 11, 2019), he explained that he had been busy due to a funeral, and STULTZ reassured the undercover that he still wanted to meet the undercover for sexual activity:

02/14/2019 11:33 AM – UC – I dunno. It feels like this is just pretend for you or something.

02/14/2019 11:36 AM – UC – Like you are just playing on me being young and dont really care about me or my feelings.

02/14/2019 11:36 AM – UC – Maybe in wrong but thays just what it feels like

02/14/2019 12:25 PM – STULTZ – TBH. I actually am keeping in mind your feelings. This isn't pretend at all. I'm actually very interested in meeting you. I truly think it's hot that you want to explore and very happy that you've considered me to help you explore (Note: In the texting context your affiant knows that TBH means "to be honest").

02/14/2019 12:26 PM – UC – Oh. Thanks. What do you mean explore?

02/14/2019 12:29 PM – STULTZ – Like, explore your sexuality

The second meeting (originally set for February 20, 2019) was called off by the undercover for a reason indicative of the minor's purported young age (mom staying home from work because of

bad weather so the minor could not skip school). After each break in contact, STULTZ reinitiated communication with the undercover and discussed plans to meet.

20. While making plans to meet, STULTZ told the undercover that he was unable to drive (law enforcement is aware that STULTZ' driver's license is suspended), and STULTZ stated that he could take the "T" (public transit) to meet the undercover at the Station Square stop. For example, on February 18, 2019, STULTZ suggested: "Station square? And then it's a 30 min bus ride to my place." But as they discussed how long the travel would take, STULTZ suggested: "I could get you a Lyft to the T though." In discussing the Lyft (car transportation) option, STULTZ later offered: "We could take it both ways." When the undercover responded: "Its up to you. I feel bad like making you pay for stuff", STULTZ responded: "It's not too expensive and worth it to meet you."

21. In a subsequent conversation on or about Friday 19, 2019, STULTZ confirmed that he and the purported 14-year-old make would ride together back from the Station Square T stop to STULTZ house together, via Lyft, and afterwards "I could get you a Lyft to the T though: Lyft will get you there in 10 minutes hehe".

22. Throughout the text conversation, STULTZ stated what he would like to do to the undercover (February 14, 2019): "make out with you, maybe try to see if your able to sit down on me and get my whole dick inside of you" and "Oh yes. I'll only go slow. I'd want it to feel good for you. Especially your first time" and "Especially if you let me cum inside of you". STULTZ also stated: "I've been told that my cock feels amazing and that my bottom could feel my cock twitch and shoot inside and then it gets really really wet in there". STULTZ informed that he had a boyfriend whom he lived with and suggested "Maybe you might eventually be down with playing with my bf and I together" and "You could be in him while I'm in you".

STULTZ then told the undercover to “Say your 16 almost 17 haha” when the undercover meets STULTZ’s boyfriend.

23. On or about February 25, 2019, STULTZ contacted the undercover and discussed meeting on Wednesday February 27, 2019 at or around 10:00 AM at Station Square. STULTZ planned on taking a Lyft to Station Square, meeting the purported 14-year-old boy at the T station (public transit), then taking a Lyft together back to STULTZ’s residence. STULTZ again suggested “just like kissing, or touching, sucking or else”.

24. On the day of the proposed meet, February 27, 2019 STULTZ did not reach out to the undercover and no contact was made. The undercover sent an emoji to STULTZ on February 27, 2019 after the proposed meeting time of 10:00 AM because he had not heard from STULTZ since February 25, 2019. STULTZ did not show up at Station Square. STULTZ did not respond and no contact was made until March 2, 2019, when STULTZ sent the undercover a message “Hey”. The undercover did not respond until March 4, 2019 and stated “Go away you really hurt me”.

25. On March 17, 2019 STULTZ reached back out to the undercover with “Hi”, “How was your weekend?” The undercover did not respond to STULTZ. On March 19, 2019 STULTZ reached back out to the undercover with an emoji followed by “Hi”. The undercover again did not respond. On March 27, 2019 STULTZ reached back out to the undercover for a third time and stated “Hey man. I haven’t heard from you in a while. I hope things are going well and just wanted to see what you were up to.”

26. On April 2, 2019, the undercover responded to STULTZ and stated “Hi”, “Sorry. My mom couldn’t pay the phone bill until April 1 or something so I couldn’t use my phone.” STULTZ replied: “Hey man. I thought you were mad at me and done talking. Haha”; “How’re

you doing?” During the conversation, STULTZ asked the undercover for a picture of his face. The undercover sent to STULTZ a sanitized picture of another law enforcement officer taken when the officer was a prepubescent boy / approximately 14 years old, to which STULTZ replied: “You’re very cute.” STULTZ then sent an image of himself without a shirt on wearing glasses. STULTZ also asked the undercover when he will be free to “Meet up. Maybe hang out haha”. STULTZ offered: “I could meet you downtown or wherever you feel comfortable”; “Go back to my place maybe?”

27. STULTZ and the undercover continued to discuss meeting on Friday (April 5, 2019). When the undercover asked STULTZ about what would happen when they met, STULTZ stated: “I’m down to try anything. But first checking out each other’s bodies and becoming familiar with them. Then trying stuff like rubbing, kissing, sucking”; “well, after we get that far I might like to show you what it’s like to have someone lick around and inside your little hole”. STULTZ then stated he “would love to show you and teach you new stuff, like getting your dick sucked. You sucking a big dick for instance, getting your pink little hole eaten out, and maybe getting a hard dick inside of it”. STULTZ confirmed he will have condoms and lube ready at his house, however, STULTZ also stated: “But I can say that bare skin will feel better your first time and be easier to get in”. STULTZ also stated: “But I know that you’d love to feel me cumming inside of you”. STULTZ and the undercover continued to discuss meeting on Friday, and made plans to meet at Station Square. STULTZ told the undercover they could take a “Bus or Lyft. Could bus there and I could Lyft you back, I’d come meet you and travel the rest of the way to my place with you”. STULTZ then stated: “Hehe I’m excited too. I might have to jerk to your picture hehe”.

28. On April 4, 2019, STULTZ reached out to the undercover and stated “Hey there”. STULTZ engaged the undercover in casual conversation about school and sports.

29. In the morning of April 5, 2019, the undercover sent STULTZ an emoji, to which STULTZ responded and asked the undercover what he was going to do today. The undercover texted STULTZ words to the effect of: Don’t know – you tell me. At that point, STULTZ asked the undercover to meet up. STULTZ made arrangements to meet with the undercover later that morning at the “T” stop at the North Shore (located next to Heinz Field). STULTZ continued to text the undercover while he was on his way, sending “selfies” and giving the undercover updates on his location. During this conversation, STULTZ texted the undercover words to the effect of: I’m also a little nervous being that your so young lol.

30. STULTZ informed the undercover when he had gotten off of the bus. The undercover told STULTZ that he was near Heinz Field. STULTZ texted the undercover that he would be there soon. When STULTZ arrived in the vicinity of Allegheny Avenue, between the intersection of Ridge Avenue and Reedsdale Street, agents placed STULTZ under arrest for violations of Title 18 U.S.C. 2422(b) and a Criminal Complaint was filed at Crim. No. 19-MJ-00749.

31. Agents seized STULTZ’s phone search incident to arrest, and STULTZ gave agents verbal and written consent to review his phone. Agents also subsequently obtained a search warrant for STULTZ’s cellular telephone, a Google Pixel 2XL corresponding to telephone number (724) 321-2360, as well as his residence (601 Bellevue Terrace, Pittsburgh, PA 15202)—both warrants were signed by Chief U.S. Magistrate Judge Cynthia Reed Eddy on April 5, 2019. During execution of the search warrant at STULTZ’s residence, agents seized a laptop computer (Alienware laptop displaying product key: CY96D-3PVJ8-2Y7WF-3G4WJ-

GQB8) in the front living room of the residence. The other resident of the apartment, who was present for the search, confirmed that this laptop belonged to STULTZ. Additionally, during the course of chatting with the undercover, STULTZ told the undercover that he does computer work from home and sent the undercover a picture of himself in a room resembling the living room of the residence where agents recovered the laptop.

32. Between the dates of April 5, 2019 and April 17, 2019, your affiant reviewed the contents of STULTZ's cellular telephone. During the review of the cellular telephone, your affiant discovered images of apparent child pornography in violation of Title 18 U.S.C. § 2252(a)(4)(b), which makes it a crime to knowingly possess a visual depiction of a minor engaged in sexually explicit conduct. These images are only located on the phone's SD card as thumbdata of the cellular telephone, and may have been deleted by the user. Thumbdata files are generated in the DCIM folder where the digital camera saves photos. Thumbdata files are used for indexing and caching and contain thumbnails of processed images.

33. STULTZ has the Grindr application on his cellular telephone. Grindr runs on iOS and Android devices, and is available for download from the Apple App Store and Google Play. While Grindr is more easily accessible on cellular telephones, it can also be downloaded onto a desktop or laptop computer and utilized with emulator hardware or software. Once the emulator is installed, the Grindr application can then be installed and used on the desktop/laptop and will function in the same way as it would on a cellular telephone.

34. All of the above facts and circumstances, taken together, lead your affiant, based on her training and experience, to believe that evidence of the offenses under investigation is located, stored, or contained on the laptop computer seized from STULTZ's residence and currently stored at FBI Pittsburgh.

DEFINITIONS

35. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. “Minor,” as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.
- b. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- c. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in “sexually explicit conduct,” as that term is defined in 18 U.S.C. § 2256(2).
- d. “Visual depictions” include undeveloped film and videotape, data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual

image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

- e. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- f. “Illicit Sexual Conduct”, as used herein, means (1) a sexual act (as defined in section 2246) with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States; or (2) any commercial sex act (as defined in section 1591) with a person under 18 years of age.
- g. “Wireless telephone”: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text

messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- h. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- i. “Digital camera”: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- j. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media

player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- k. “Internet Service Providers” or “ISPs,” are businesses that enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines, provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers, remotely store electronic files on their customers’ behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.
- l. An “Internet Protocol” or “IP” address is a unique numeric address used by computers or cellular telephones on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by

periods (e.g., 121.56.97.178). Every computer connected to the Internet must have an assigned IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the computer an IP address. Any and all computers using the same ISP account during that session will share an IP address. The customer's computer retains the IP address for the duration of the Internet session until the user disconnects. The IP address cannot be assigned to a user with a different ISP account during that session. When an Internet user visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

- m. "Internet": The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

36. Based on my training, experience, and research, I know that the cellular telephones, have capabilities that allow it to serve as a wireless telephone, computer, digital camera, and portable media player. I also know that laptop computers, desktop computers, and hard drives allow for the storage of large amounts data, including internet browsing histories, documents, images, and videos. They also function as a repository for backing up data from

cellular telephones, namely images and video files. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

37. In my training and experience, I know that computers and electronic mobile devices essentially serve four functions in connection with child pornography: (1) production; (2) communication; (3) distribution; and (4) storage.

38. Child pornographers can now easily transfer existing hard copy photographs into a computer-readable format with a scanner. With the advent of digital cameras, images can be transferred directly from the digital camera onto an electronic mobile device or a computer. Moreover, a device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

39. The Internet affords collectors of child pornography several different venues for obtaining viewing and distributing child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by internet portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or device with access to the Internet. Evidence of such online storage of child pornography is often found in the user's computer.

40. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. Digital devices connected to the Internet can provide access to large amounts of storage associated with “cloud storage.” “Cloud storage” allows data to be accessed, managed, and maintained from a network, usually the Internet. Identification of an individual’s access and use of “cloud storage” can be identified by forensically reviewing a digital device.

41. With the advent of smart phones and advanced technology, cellular telephones and other electronic mobile devices function as “computers” in the sense that they can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. In fact, some cellular telephones are equipped with memory or SIM cards, which are compact removable storage devices commonly used to store images and other electronic data that can be inserted into a telephone’s camera as well as other small digital devices such as tablet devices or hand held computers. Much like “thumb drives,” some memory cards have the ability to store large amounts of electronic data, including thousands of images or videos, and on occasion entire operating systems or other software programs. Moreover, cellular telephones offer a broad range of capabilities. In addition to enabling voice communications and containing a “call log” that records phone call details, cellular telephones offer the following capabilities: storing names and phone numbers in electronic “address books;” sending receiving, and storing text messages and e-mails; taking, sending, receiving, and storing still photographs and moving videos; storing and laying back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

42. Communications made by way of computer or electronic mobile devices can be saved or stored on the items used for these purposes. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or electronic mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally. For example, traces of the path of an electronic communication may be automatically stored in many places like temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer or electronic mobile device contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

43. Computer and electronic mobile device users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer and electronic mobile device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer and electronic mobile device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." By using steganography, a computer or electronic mobile device user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to

extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

44. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or other electronic storage media, deleted or viewed via the Internet. Electronic files saved to a hard drive or electronic storage media can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer or electronic mobile device, the data contained in the file does not actually disappear; rather, that data remains on the hard drive or electronic storage media until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (i.e., space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten).

45. In addition, a computer's (or electronic mobile device's) operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive or electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer or electronic mobile device habits. A substantial amount of time is necessary to extract and sort through data in this free or unallocated space.

46. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computers and electronic mobile devices can contain other forms of electronic evidence as well. In particular, records of how a computer or electronic mobile device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the computer and electronic mobile devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that can be neatly segregated from the hard drive image as a whole. Digital data on the hard drive or electronic storage media not currently associated with any file can provide evidence of a file that was once on the hard drive or electronic storage media but has since been deleted, edited, or deleted in part such as a word processing file with a deleted paragraph. Virtual memory paging systems can leave digital data on the hard drive or electronic storage media that show what tasks and processes on the computer or electronic storage media were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive or electronic storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer or electronic mobile device was in use. Computer file systems (or those on electronic mobile devices) can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN
CHILD PORNOGRAPHY AND WHO HAVE A
SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN**

47. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who create, view, or receive visual depictions of minors engaged in sexually explicit conduct are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

- a. Such individuals almost always possess and maintain their “hard copies” or “digital copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- b. Likewise, such individuals often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or electronic mobile device. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection, which is valued highly.
- c. Such individuals also may correspond with and/or meet others to share

information and materials; rarely destroy correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- d. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

FORENSIC ANALYSIS

48. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on each device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited; Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web

browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled a device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence;
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when;
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

50. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

51. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION


52. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2422(b), 2251(a), 2252(a)(2) and 2252(a)(4)(B) may be located in the device located at FBI Pittsburgh (more fully described in Attachment A).

53. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

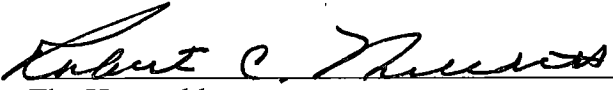
54. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the Application, Affidavit, and the Search Warrant, and the requisite inventory notice (with the exception of one (1) copy of the warrant and inventory notice that will be left with the evidence

at HSI Pittsburgh. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact of this continuing investigation and may jeopardize its effectiveness.

55. The above information is true and correct to the best of my knowledge, information and belief.


KATHERINE DONOHUE
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 19th day of April 2019.


The Honorable
United States Magistrate Judge

ATTACHMENT A

The property to be searched is currently located at Federal Bureau of Investigation (FBI) Pittsburgh, located at 3311 E Carson St, Pittsburgh, PA 15203. The item is listed specifically, below.

This warrant authorizes the forensic examination of the device for the purpose of identifying the electronically stored information described in Attachment B.

- One (1) Alienware laptop displaying product key: CY96D-3PVJ8-2Y7WF-3G4WJ-GQB8

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Sections 2242(b), 2251(a), 2252(a)(2) and 2252(a)(4)(B) and involve THOMAS PERRY STULTZ and constitute evidence of or pertain to an interest in child pornography (possession/receipt/distribution/production) or sexual activity with children, and the aiding and abetting of these crimes, including:

- a. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- b. Child erotica and evidence of access to children;
- c. Information, correspondence, records, documents, or other materials constituting evidence of or pertaining to child pornography, child erotica, or access to children; or constituting evidence of or pertaining to the production, possession, receipt, distribution, accessing, or transmission through interstate or foreign commerce of child pornography, child erotica, or visual depictions of minors engaged in sexually explicit conduct; or constituting evidence of or pertaining to an interest in child pornography or sexual activity with children, to include but not limited to chatting or social networking applications (“APPs”) which can be used to communicate with minors, such as Grindr, as well as ingoing and outgoing message logs and contact lists; photo and video galleries; online or electronic communications sent and received, including email, chat, and instant messages, as well as messages drafted but not sent; sent and received audio files; and P2P software;

2. For the SUBJECT DEVICE further described in Attachment A whose seizure is otherwise authorized by this warrant:

- a. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the SUBJECT DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence, including evidence of online storage or other remote electronic or “cloud” storage, including, but not limited to, software used to access such online storage or remote electronic or “cloud” storage, user logs or archived data that show connection to such online storage or remote electronic or “cloud” storage, and user logins and passwords for such online storage or remote electronic or “cloud” storage.
- e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

- f. Evidence of the times the DEVICE was used;
- g. Records of or information about Internet Protocol addresses used by the DEVICE;
- h. Records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- i. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form (such as prints or videotapes). However, no real-time communications will be intercepted and searched during service.